Exhibit 7

ZeroAccessJP help

Started by BranDuir , Dec 04 2014 03:44 PM

BranDuir

Posted 04 December 2014 - 03:44 PM

I seem to have picked up this nasty little bugger and nothing seems to get rid of it. SpyHunter found it but I'm pennyless so can't pay for it to remove it. I'm at a loss so any help would be greatly appreciated.

Guest_LighthouseParty_*

Posted 04 December 2014 - 03:48 PM

Hello there 

I'm LighthouseParty and I'll be assisting you with your concern today. Let's run a couple of scans to see what could be causing this.

1 Download MiniToolBox

1. Click here to download MiniToolBox (http://www.bleepingcomputer.com/download/minitoolbox/) to your desktop.
2. Double click MiniToolBox.
3. Select the following and then press go.
4. Post the log in your next reply.

Flush DNS
Reset IE Proxy Settings
Reset FF Proxy Settings
List Installed Programs
List Restore Points

2 Install and run a scan with Malwarebytes Anti-Malware

1. Click here (https://www.malwarebytes.org/mwb-download/) to download Malwarebytes to your desktop.
2. Double click mbam-setup-x.x.x.xxxx and follow the on-screen instructions.
3. On the dashboard, click update now.
4. After that, click scan now - the scan will now begin.

5. When the scan's completed, select apply actions - make sure the action is quarantine.
6. Restart your computer.

How to get the log.

1. On the dashboard, select the history tab and click application logs.
2. Select the log which has the time and date of when you did the scan.
3. Click copy to clipboard and paste it into your reply.

Download Security Check

1. Click here (http://www.bleepingcomputer.com/download/securitycheck/) to download Security Check to your desktop.
2. Double click SecurityCheck and follow the on-screen instructions.
3. A log should open, called checkup.txt.
4. Please post the contents of it in your next reply.

Thanks and good luck!

quietman7

Posted 04 December 2014 - 04:57 PM

SpyHunter by Enigma Software Group (ESG) is a program that was previously listed as a **rogue product** on the **Rogue/Suspect Anti-Spyware Products List (http://spywarewarrior.com/de-listed.htm#sh_note)** because of the company's history of employing **aggressive and deceptive advertising**. It has since been delisted but Enigma still engages in deceptive advertising which violates several consumer protection laws in many states. In my opinion it is a **dubious program** which is not very effective compared to others with a proven track record and I would not trust all the detections provided by its scanning engine.

AV-Test (http://www.av-test.org/en/tests/test-reports/) has not beem able to include SpyHunter in their comprehensive testing analysis which would reveal how SpyHunter compares to anti-spyware competitors in terms of protection, detection, repair and usability. The reason for this is that the publisher, Enigma Software, **has not been cooperative in submitting SpyHunter for testing** at AV-Test...most likely due to the program's ineffectiveness and high rate of false positives (http://antivirus.about.com/library/glossary/bldef-false.htm).

While there are mixed reviews for SpyHunter, many customers have reported deceptive pricing, continued demands for payment after requesting a refund, lack of adequate customer support, removal (uninstall) problems and various other issues with their computer as a result of using this product. Newer versions of SpyHunter apparently install it's own "Compact OS" and uses Grub4Dos loader to execute on boot up. The user no longer sees the normal Windows boot menu but instead sees the GRUB menu. For some folks this has resulted in SpyHunter causing a continuous loop when attempting to boot and other issues. You may want to read some of the user comments posted on the Complaints Board: Enigma Software Group Spyhunter Complaints & Reviews (http://www.complaintsboard.com/complaints/enigma-software-group-spyhunter-c262520.html).

Further, when searching for new malware or malware removal assistance (and removal guides) on the Internet, **it is not unusual to find numerous hits from untrustworthy and scam** sites which misclassify detections or provide **misleading information**. This is deliberately done more as a **scam** to entice folks into buying an advertised fix or using a free removal tool. **SpyHunter** (SpyHunter-Installer.exe) is one of the most common "so-called" removal tools pushed by these sites.

- SpyHunter - Fake security blogs (http://en.kioskea.net/faq/31535-spyhunter-fake-security-blogs)

.
If you have downloaded and scanned with SpyHunter, any **detection results should be viewed with suspicion**. My personal recommendation would be to remove the program and replace it with a trustworthy alternative such as Malwarebytes Anti-Malware (https://www.malwarebytes.org/antimalware/) or Emsisoft Anti-Malware (http://www.emsisoft.com/en/software/antimalware/).

- How to Uninstall SpyHunter (http://www.enigmasoftware.com/spyhunter-uninstall-steps/)

.
*Note: Some users have reported that you may need to open Windows Explorer, navigate to the following location, look for and delete a SpyHunter related file named **SHSetup.exe** before uninstalling from Programs and Features (Add/Remove Programs) in Control Panel.*

*-- **XP**: C:\Documents and Settings\<user name>\Local Settings\Temp*
*-- **Vista, Windows 7/8**: C:\Users\<user name>\AppData\Local\Temp*

quietman7

Posted 04 December 2014 - 04:59 PM

[ZeroAccess rootkit (https://nakedsecurity.sophos.com/zeroaccess2/)](https://nakedsecurity.sophos.com/zeroaccess2/) is a serious malware infection. If that is what you actually have, then **disinfection will probably require the use of more powerful tools than we can recommend in this forum**.

Hold off on following LighthouseParty's instructions.

Please download **[RKill (http://www.bleepingcomputer.com/download/rkill/)](http://www.bleepingcomputer.com/download/rkill/)** by Grinler and save it to your desktop.

- Double-click on the **Rkill** desktop icon to run the tool.
  Vista/Windows 7/8 *users right-click and select [Run As Administrator (http://windows.microsoft.com/en-US/windows7/How-do-I-run-an-application-once-with-a-full-administrator-access-token)](http://windows.microsoft.com/en-US/windows7/How-do-I-run-an-application-once-with-a-full-administrator-access-token).*
- A **black DOS box** will briefly flash and then disappear. This is normal and indicates the tool ran successfully.
- A log file will be created and saved to the root directory, C:**RKill.log**
- Copy and paste the contents of **RKill.log** in your next reply.

BranDuir

Posted 05 December 2014 - 07:39 AM

For quietman7

As requested the contents of the RKill.log:

Rkill 2.6.8 by Lawrence Abrams (Grinler)
[http://www.bleepingcomputer.com/ (http://www.bleepingcomputer.com/)](http://www.bleepingcomputer.com/)
Copyright 2008-2014 BleepingComputer.com
More Information about Rkill can be found at this link:
[http://www.bleepingcomputer.com/forums/topic308364.html (http://www.bleepingcomputer.com/forums/topic308364.html)](http://www.bleepingcomputer.com/forums/topic308364.html)

Program started at: 12/05/2014 12:34:19 PM in x64 mode.
Windows Version: Windows 7 Home Premium Service Pack 1

Checking for Windows services to stop:

* No malware services found to stop.

Checking for processes to terminate:

* No malware processes found to kill.

Checking Registry for malware related settings:

* No issues found in the Registry.

Resetting .EXE, .COM, & .BAT associations in the Windows Registry.

Performing miscellaneous checks:

* Windows Firewall Disabled

[HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile]
"EnableFirewall" = dword:00000000

* ALERT: ZEROACCESS rootkit symptoms found!

* C:\Program Files (x86)\Google\Desktop\Install\{0c17f446-b9c1-bbe0-744f-43ffe625f916}\ [ZA Dir]
* C:\Program Files (x86)\Google\Desktop\Install\{0c17f446-b9c1-bbe0-744f-43ffe625f916}\ \ [ZA Dir]
* C:\Program Files (x86)\Google\Desktop\Install\{0c17f446-b9c1-bbe0-744f-43ffe625f916}\ \...\ [ZA Dir]
* C:\Program Files (x86)\Google\Desktop\Install\{0c17f446-b9c1-bbe0-744f-43ffe625f916}\ \...\سئى\ [ZA Dir]
* C:\Program Files (x86)\Google\Desktop\Install\{0c17f446-b9c1-bbe0-744f-43ffe625f916}\ \...\سئى\ {0c17f446-b9c1-bbe0-744f-43ffe625f916}\ [ZA Dir]

Checking Windows Service Integrity:

* PcaSvc [Missing Service]
* PolicyAgent [Missing Service]
* RemoteAccess [Missing Service]

Searching for Missing Digital Signatures:

* No issues found.

Checking HOSTS File:

* No issues found.

Program finished at: 12/05/2014 12:35:59 PM
Execution time: 0 hours(s), 1 minute(s), and 40 seconds(s)

Thank you for your help on this matter.

quietman7

Posted 05 December 2014 - 08:53 AM

> *Quote*
>
> *** ALERT: ZEROACCESS rootkit symptoms found!**

You will need to create and post a DDS log for further investigation.

Please follow the instructions in the **Malware Removal and Log Section Preparation Guide (http://www.bleepingcomputer.com/forums/t/34773/preparation-guide-for-use-before-using-malware-removal-tools-and-requesting-help/)** starting at Step 6.

- **If you cannot complete a step, then skip it and continue** with the next.
- In **Step 6** there are instructions for downloading and running **DDS** which will create two logs. (Note: Windows 8.1 Users will not be able run DDS and create a log)

When you have done that, **post your logs** in the Virus, Trojan, Spyware, and Malware Removal Logs forum (http://www.bleepingcomputer.com/forums/f/22/virus-trojan-spyware-and-malware-removal-logs/), **NOT here**, for assistance by the Malware Response Team.

Start a new topic, give it a relevant title and post your log(s) along with a brief description of your problem, a summary of any anti-malware tools you have used and a summary of any steps that you have performed on your own. If you cannot produce any of the required logs or you're using Windows 8.1, then still start the new topic and explain that you followed the Prep. Guide, were unable to create the logs, and describe what happened when you tried to create them. A member of the Malware Removal Team will walk you through, step by step, on how to clean your computer.

After doing this, please reply back in this thread with a link to the new topic so we can close this one.

Back to Am I infected? What do I do?